

**METHOD OF AUTHENTICATING CONTENT PROVIDER AND
ASSURING CONTENT INTEGRITY**

BACKGROUND

[01] This application claims the priority of Korean Patent Application No. 10-2003-0029144 filed on May 7, 2003 in the Korean Intellectual Property Office, the disclosure of which is incorporated herein in its entirety by reference.

1. Field of the Invention

[02] The present invention relates to a method of authenticating a content provider and assuring content integrity, and more particularly, to a method of authenticating a content provider and assuring content integrity by which the content provider is authenticated and content integrity is assured upon download, exchange, or transfer of a variety of multimedia contents through a wired/wireless communication network.

2. Description of the Related Art

[03] Recently, a variety of contents are distributed through wired/wireless communication networks, and development of a variety of techniques has been actively made to protect the copyrights of digital contents. A typical technique includes Digital Rights Management (DRM), for example, which encompasses DRM and Open Mobile Alliance (OMA) DRM v1.0 of Microsoft Corporation.

Q80013 - SPECIFICATION TO BE FILED

[04] In a case where a user utilizing a device with the DRM function downloads packaged contents, sends such contents to a device of another user, or freely exchanges and sends them through a bulletin board or by e-mail via a wired/wireless communication network, there is a technique to assure the integrity of the contents sent.

[05] FIG. 1 shows the configuration of conventional packaged contents 1. The contents 1 comprises an encrypted content portion 2, a header 3 including a variety of information on the relevant contents, and an electronic signature 4 made through hash coding of the header 3 of the contents 1. As shown in FIG. 1, the content portion 2 is encrypted and the header 3 includes the content provider's (CP's) name, a content ID, meta-information, the license provider's URL and the like. Here, a hash function is generally utilized in the electronic signature 4. The hash function can be described as a computationally effective function that performs mapping of an arbitrary-size binary string to a fixed-size binary string that is called a hash value. Such a hash function can be used to ensure data integrity in addition to its use for the electronic signature 4.

[06] For example, when the contents 1 including the electronic signature 4, made through the beforehand hash coding of the header 3 of the contents 1, are downloaded, a hash function is then applied to the contents 1 and the electronic signature 4 is compared with a public key provided by the content provider so as to verify the electronic signature.

Q80013 - SPECIFICATION TO BE FILED

[07] In such a case where a user downloads the packaged contents 1 from a content provider or receives them from another user through a wired/wireless communication network, the encrypted content portion 2 is transmitted together with the header 3 having the electronic signature 4 made through the beforehand hash coding of the header 3. Thus, the integrity of the packaged contents 1 is assured.

[08] However, according to such related art, the electronic signature 4 is made through the hash coding of only the header 3. Thus, there is a problem in that the integrity of mutual connectivity of the encrypted content portion 2 and the header 3 cannot be assured.

[09] Further, there are problems in that it is impossible to authenticate whether the received contents 1 were prepared by a legitimate content provider, and in that there is no way to acquire a public key certificate of a content provider required for verifying the integrity of the packaged contents 1.

SUMMARY

[10] The present invention is conceived to solve the aforementioned problems in the prior art. An aspect of the present invention is to provide a method of authenticating a content provider and assuring content integrity, wherein a header of contents comprises a uniform resource locator (URL) address enabling acquisition of a certificate of the content provider so as to acquire the certificate of the content provider, thereby verifying an electronic signature.

Q80013 - SPECIFICATION TO BE FILED

[11] Consistent with an aspect of the present invention for achieving the object, there is provided a packaged content structure for authenticating a content provider and assuring content integrity, comprising an encrypted content portion and a header comprising an address from which a certificate of the content provider can be acquired.

[12] Consistent with another aspect of the present invention, there is provided a method of authenticating a content provider and assuring content integrity, comprising downloading packaged contents with an electronic signature made thereto into a device of a user through a wired/wireless communication network, finding a URL address from which a certificate for verification of the signature of the content provider is provided, in a header of the contents, acquiring the certificate of the content provider after moving to the URL address, extracting a public key required for verification of the electronic signature from the acquired certificate, and verifying the electronic signature by using the extracted public key.

BRIEF DESCRIPTION OF THE DRAWINGS

[13] The above and other aspects, features and advantages of the present invention will become apparent from the following description of an exemplary embodiment given in conjunction with the accompanying drawings, in which:

[14] FIG. 1 is a view showing the configuration of conventional packaged contents;

Q80013 - SPECIFICATION TO BE FILED

[15] FIG. 2 is a view showing the configuration of packaged contents consistent with the present invention;

[16] FIG. 3 is a block diagram showing the process of authenticating a content provider consistent with the present invention; and

[17] FIG. 4 is a flowchart illustrating a method of authenticating a content provider and assuring content integrity consistent with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[18] Hereinafter, an exemplary embodiment of the present invention will be described in detail in view of its object and constitution with reference to the accompanying drawings.

[19] FIG. 2 is a view showing the configuration of packaged contents 10 consistent with the present invention. As shown in FIG. 2, the contents 10 comprises an encrypted content portion 11, a header 12 including an address enabling acquisition of a certificate of a content provider 20 (see Fig. 3) and a variety of information on the relevant contents, and an electronic signature 13 for assuring the integrity of the contents.

[20] The header 12 includes the name of the content provider (CP) 20 distributing the contents to users, a content ID, a license provider's URL, meta-information, a URL address enabling the acquisition of the certificate of the content provider 20, and the like. Here, the header is characterized by the URL address providing the certificate of the content provider 20. The certificate of the

Q80013 - SPECIFICATION TO BE FILED

content provider 20 can be acquired through the URL address, so that it is possible to verify whether the content provider 20 is the same provider that has provided the relevant contents.

[21] To assure the integrity of the packaged contents 10 and to authenticate the content provider 20, the content provider 20 inserts the electronic signature 13 made through hash coding of the header 12 and the encrypted content portion 11 into the packaged contents 10. If it is difficult to make the electronic signature 13 through the hash coding due to the large size of the encrypted content portion 11, only a portion of the encrypted content portion 11 is hash coded and then used together with the header 12 to make the electronic signature.

[22] FIG. 3 is a block diagram showing the process of acquiring the certificate of the content provider 20 by using information of the header 12 of the packaged contents 10.

[23] The content provider 20 performs the hash coding of the header 12 and the encrypted content portion 11, inserts the resultant electronic signature 13 into the packaged contents 10, and provides a public key (not shown) required for verification of the electronic signature 13 to the certificate received beforehand from a relevant certification authority (CA) 30. When a user B downloads the contents 10 from the content provider (CP) 20 or a user A, the user acquires the certificate of the content provider 20 by using the URL address from which the certificate of the content provider 20 is provided, and extracts the public key.

Q80013 - SPECIFICATION TO BE FILED

Then, the electronic signature 13 is verified by comparing the value of the public key with a hash value obtained through the hash coding of the contents 10. Thus, authentication of the content provider 20 can be made and the integrity of the contents 10 can be assured.

[24] FIG. 4 is a flowchart illustrating the method of authenticating the content provider 20 and assuring content integrity, which is performed through a wired/wireless communication network in a device with a DRM function. Here, to exchange and transfer a variety of multimedia contents through an existing communication network, the content provider 20 generally has its own certificate, which has been already certificated as an electronic signature by the certification authority 30, and has beforehand used the public key in verifying the certificate of the content provider 20. In this case, how a user verifies the packaged contents 10 will be described.

[25] First, the packaged contents to which the electronic signature is made through the hash coding of the header and the encrypted content portion are downloaded into the user's device via the wired/wireless communication network (S10).

[26] Then, the URL address from which the certificate of the content provider 20 for verifying the signature is provided is found in the header 12 of the downloaded contents 10 (S20).

Q80013 - SPECIFICATION TO BE FILED

[27] After the URL address is found, movement to the URL address is made to acquire the certificate of the content provider 20 (S30).

[28] Next, the public key required for verification of the electronic signature 13 is extracted from the acquired certificate of the content provider 20 (S40).

[29] Then, the electronic signature is verified by using the extracted public key (S50).

[30] If the verification is successfully made in the verification step (550), the integrity of the mutual connectivity of the header 12 and the encrypted content portion 11 is assured and the content provider 20 is authenticated as a legitimate content provider.

[31] The step of verifying the electronic signature 13 may comprise applying a hash function to the packaged contents 10 and performing a comparison with the electronic signature 13.

[32] Further, the electronic signature 13 is made through the hash coding of the header 12 and the encrypted content portion 11 and then inserted into the contents 10. In this case, all or some of the encrypted content portion 11 may be hash coded.

[33] A hash value obtained by applying the hash function to the contents 10 is compared with the value of the extracted public key to verify the electronic signature.

Q80013 - SPECIFICATION TO BE FILED

[34] As described above, the certificate of the content provider 20 is acquired by referring to the header 12 of the packaged contents 10 and then used for verifying the electronic signature 13. Thus, the integrity of the contents 10 can be verified and the content provider 20 can be authenticated.

[35] Consistent with the present invention , a content receiver can confirm receipt of the contents by verifying the integrity that assures the connectivity of the header and the encrypted content portion. Further, there are advantages in that authentication can be made that the contents were provided by a legitimate content provider, and in that the integrity of the contents can be verified by verifying the electronic signature based on the hash value of the packaged contents.

[36] Although the present invention has been described in detail in connection with an exemplary embodiment of the present invention, it will be apparent to those skilled in the art that various changes and modifications can be made thereto without departing from the spirit and scope of the invention defined by the appended claims. Thus, various modifications to the exemplary embodiment of the present invention fall within the scope of the present invention.